

United States District Court
Eastern District of Michigan
Southern Division

United States of America,

Plaintiff,

Case No. 19-20008

v.

Honorable Judith E. Levy

Jonathan Woods,

Defendant.

United States's Sentencing Memorandum

Jonathan Woods committed wire fraud on a large scale by posing as a proficient and lucrative credit card scammer and fraudster. Under the moniker “Selfmade Kash,” Woods brazenly boasted of his supposed credit card fraud prowess in rap song videos and photographs on social media platforms such as YouTube, Twitter, and Instagram. To give credence to his alleged scamming prowess, Woods posted pictures depicting him living a lavish lifestyle supposedly resulting from credit card fraud.

Woods posted pictures of himself with the supposed rewards from his credit card scamming lifestyle such as large amounts of money, expensive sneakers, lavish hotel rooms, a custom made jeweled necklace

which reads “LilWillWorld” that was a tribute to his slain brother William, and drugs such as marijuana and cough syrup containing codeine—the cough syrup is mixed with pop or punch and the resulting drink is called “lean” on the streets. Woods called himself the credit card swipe or scam “GOAT” (Greatest of All Time) on social media. To lend credence to that title, Woods purchased a jeweled charm made in the image of a goat from the jewelry store Victoria Jewelry Paz in Boston, MA. (<https://www.youtube.com/watch?v=AeJdgWR7IKk>).

Woods’s postings on social media attracted wanted and unwanted attention. Because these lavish accoutrements—supposedly derived from his alleged credit card scamming—had the potential to attract envious robbers, Woods portrayed himself as ready to combat any robbers by posing with various firearms. In fact, Woods was shot in the arm while in Detroit and of course went on social media to show the flesh wound and question the fact that people were trying to kill him. (<https://www.youtube.com/watch?v=THjcHX5UR7o>). In California, Woods was robbed of his custom made “LilWillWorld” necklace. Afterwards, the robbers mocked Woods on YouTube and ransomed his

necklace by apparently overwriting the beginning of one of Woods's YouTube videos. (<https://www.youtube.com/watch?v=95P6ugOKg2U>).

Upset with the public doubting his money making prowess, or the authenticity of his money, Woods went on YouTube and bragged about making \$25,000 in a month. Woods proceeded to count out \$20,000 in actual cash (<https://www.youtube.com/watch?v=yF72fuv5Cpw>). In another video, Woods held up to the light several hundred dollar bills from a pile of money on the floor to prove they were authentic and bragged of having \$50,000 in the pile.

(<https://www.youtube.com/watch?v=scEgf-8zNqM>).

Woods's social media postings and bragging attracted people who wanted to learn the art of credit card fraud and become as proficient as Woods. Would be credit card fraudsters contacted Woods through the private chat function of various social media platforms and asked him to teach them how to become proficient at credit card fraud. However, Woods duped them and scammed them out of their money. Woods would require the putative pupils to first wire him several hundred dollars, sometimes as much as \$800 or \$1,000, under the monikers "James Green," "Tewan Dean," and either "Teela or Lateef Mealy." It

should be noted on page 15 of Woods's PreSentence Report (PSR), his girlfriend's name is "Teela Mealy." (PSR at ¶61.)

After the putative pupils wired him the money, Woods would require them to show proof by either Face Timing or texting him with a copy of the receipt. Woods would next require them to call him.

Thereafter, Woods would send them instructions to download the "Red Onion" or "TOR" (The Onion Router) browsers to access the dark web.

After Woods received payments, he also provided his followers with a starter pack of Personal Identifying Information (PII) pertaining to more than 16 people (including true names, addresses, social security numbers, email accounts, and passwords), along with login links to various websites such as Freshstuff and Skynet on the dark web known to sell "full or fullz dumps" (full or "fullz" means all of the identifying information pertaining to stolen credit card numbers listed on the site such as: an individual's name, Social Security number, birth date, account numbers, corresponding Personal Identification Numbers (PINs), and other data. Woods portrayed himself obtaining the PII from skimmers he left at gas stations that police departments supposedly

seized. Additionally, Woods suggested his followers acquire Bank Identification Numbers (BINs) from these websites.

Ultimately, Woods' followers were unable to use the information he provided because the tips Woods offered were useless as he did not, in fact, know how to commit credit card fraud despite his flaunted claims as being the "Goat." When his followers complained, Woods stopped all communication; however, he kept their money.

Because of the severity of his actions and Hill's lack of remorse, as well as to deter others engaged in this credit card fraud epidemic sweeping Detroit, the government asks for a sentence of 28 months.

I. Factual and Procedural History

A. Offense Conduct

From May 2017 to May 2018, Jonathan Woods, also known as "Selfmade Kash," portrayed himself on social media platforms (Facebook, Youtube, Instagram, and Twitter) as a rapper under the name "Selfmade Kash" and also made claims to be the greatest "swiper" of all time, meaning he was prolific at credit card fraud. Furthermore,

Woods proclaimed himself as the “Goat” of credit card fraud through his social media.

Jonathan Woods boasted on social media of his scamming prowess and flashed lots of cash. Examples of his posts are below.



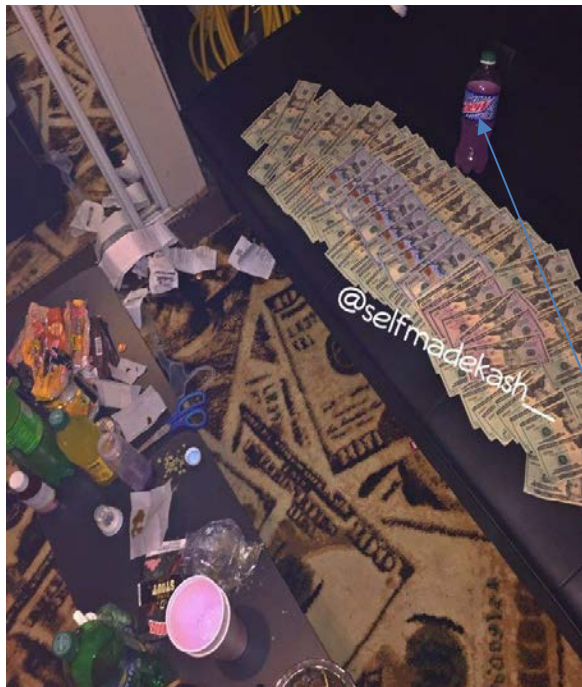
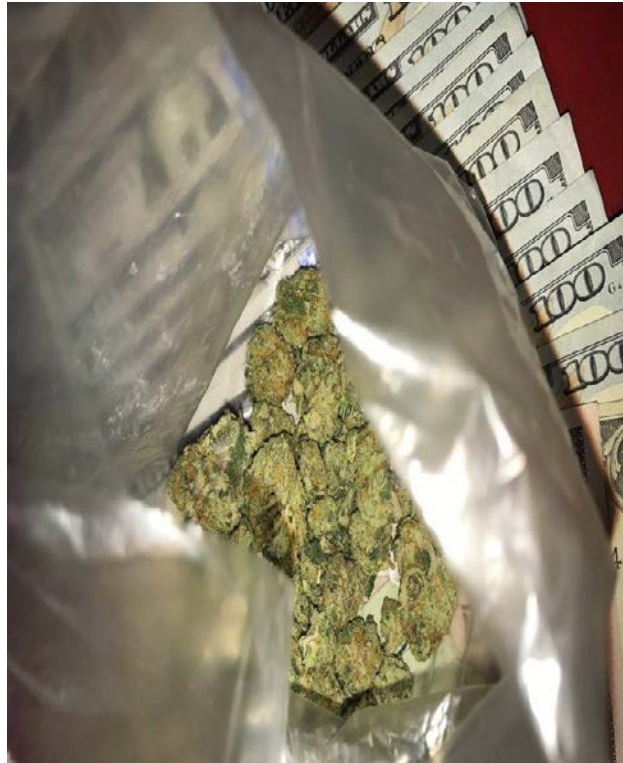
Jonathan Woods advertised for people to contact him to learn how to scam or “flip cash.”



Jonathan Woods boasted of the riches he garnered from credit card fraud such as custom jewelry, boxes of expensive sneakers in his closet, and drugs such as marijuana and lean.







Mixture of lean

Jonathan Woods had a phone number whose area code was (248) and its prefix was 866.

5/18/2018 9:57:45 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
What's up How are you

Status: Sent
Delivered: 5/18/2018 9:57:46 PM(UTC-4)
Read: 5/18/2018 9:57:51 PM(UTC-4)

5/18/2018 9:58:26 PM(UTC-4)Direction:Incoming, +1313329 [REDACTED]
I'm okay you ?what's your name

Status: Read
Read: 5/18/2018 9:58:33 PM(UTC-4)

5/18/2018 9:58:44 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
It's on my Facebook lol Jonathan

Status: Sent
Delivered: 5/18/2018 9:58:45 PM(UTC-4)
Read: 5/18/2018 9:58:49 PM(UTC-4)

5/18/2018 10:01:13 PM(UTC-4)Direction:Incoming, +1313329 [REDACTED]
I hear you when your birthday

Status: Read
Read: 5/18/2018 10:01:21 PM(UTC-4)

5/18/2018 10:01:23 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
Nov7

5/6/2018 8:08:57 PM(UTC-4)Direction:Incoming, +1626497 [REDACTED]
What's your name?

Status: Read
Read: 5/6/2018 8:08:58 PM(UTC-4)

5/6/2018 8:09:14 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
My name Jonathan but people call me kash

Status: Sent
Delivered: 5/6/2018 8:09:18 PM(UTC-4)

Jonathan Woods used that phone to text credit card information to putative pupils as well as websites on the dark web.

5/22/2018 8:15:35 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
600 night

Status: Sent
Delivered: 5/22/2018 8:15:35 PM(UTC-4)

5/22/2018 8:15:50 PM(UTC-4)Direction:Incoming, +1415470 [REDACTED]
Yea

Status: Read
Read: 5/22/2018 8:16:23 PM(UTC-4)

5/22/2018 8:16:34 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
ima have a couple sites for you see what work best

Status: Sent
Delivered: 5/22/2018 8:16:34 PM(UTC-4)

5/22/2018 8:17:26 PM(UTC-4)Direction:Incoming, +1415470 [REDACTED]
Ok

Status: Read
Read: 5/22/2018 8:20:03 PM(UTC-4)

5/22/2018 8:19:57 PM(UTC-4)Direction:Incoming, +1415470 [REDACTED]
I'm back

Status: Read
Read: 5/22/2018 8:20:03 PM(UTC-4)

5/22/2018 8:20:11 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
You got laptop?

Status: Sent
Delivered: 5/22/2018 8:20:11 PM(UTC-4)

5/22/2018 8:20:16 PM(UTC-4)Direction:Incoming, +1415470 [REDACTED]
Yea

Status: Read
Read: 5/22/2018 8:20:19 PM(UTC-4)

5/22/2018 8:20:28 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
Download a tor browser

Status: Sent
Delivered: 5/22/2018 8:20:29 PM(UTC-4)

5/22/2018 8:20:32 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
Or you got one

Status: Sent
Delivered: 5/22/2018 8:20:34 PM(UTC-4)

5/22/2018 8:20:38 PM(UTC-4)Direction:Incoming, +1415470 [REDACTED]
Got one

Status: Read
Read: 5/22/2018 8:21:51 PM(UTC-4)

5/22/2018 8:21:58 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
<https://freshstuff24.net/>

Attachments:



74B25FE6-467F-468B-BB9C-
193056B4BAF0.pluginPayloadAttachment

Status: Sent
Delivered: 5/22/2018 8:22:00 PM(UTC-4)

5/22/2018 8:23:21 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
I got the login info

Status: Sent
Delivered: 5/22/2018 8:23:22 PM(UTC-4)

5/22/2018 8:23:25 PM(UTC-4)Direction:Incoming, +1415470 [REDACTED]
OK I'm on

Status: Read
Read: 5/22/2018 8:23:30 PM(UTC-4)

5/22/2018 8:23:35 PM(UTC-4)Direction:Outgoing, +1248667 [REDACTED]
You logged in

An example of one of the 16 PII's Woods shared with each of his putative pupils.

Credit card# Credit card exp. date Home Address

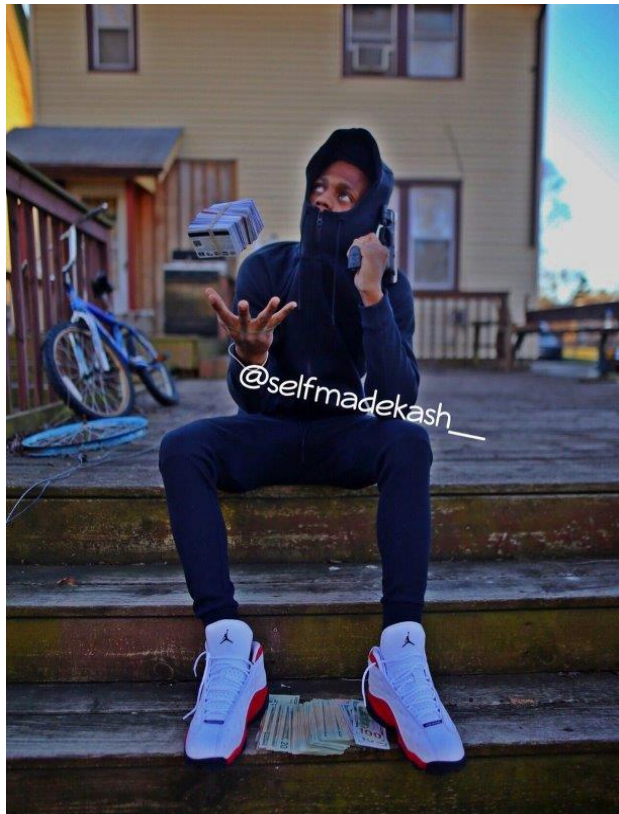
2/6/2018 10:25:59 AM(UTC-5)Direction:Outgoing, +1248667
 544856 [REDACTED] 10 / 19|026|DeRobert Adams| [REDACTED] Jackson st||Murfreesboro |Tennessee|38019|United
 States|9014126531|DoB:6/2/19 [REDACTED] 34)|SIN/SSN:279 [REDACTED] Sort C:|Bank Acc #:|Driving License
 Num:0902 [REDACTED] Cantar [REDACTED] @hotmail.com|E [REDACTED]

Status: Sent
 Delivered: 2/6/2018 10:26:00 AM(UTC-5)

Driver's license number Date of Birth Social Security Number

Personal email and password

Jonathan Woods possessed firearms.



Jonathan Woods gave the appearance he lived the proverbial high life and received luxurious hotel accommodations as a result of credit card swiping.



B. Procedural History

On January 3, 2019, a six-count Indictment was filed, under seal, under Docket Number 5:19-CR-20008. The Indictment charged Jonathan Woods with Count 1-4: Wire Fraud, in violation of 18 U.S.C. § 1343; and Count 5: Possession of Fifteen or More Unauthorized Access

Devices, in violation of 18 U.S.C. § 1029(a)(3). Count 6 charged Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A(a)(1). According to the Indictment, Counts 1 through 4 began in or about May 2017 and continued to in or about May 2018, the exact dates being unknown, in the Eastern District of Michigan. Counts 5 and 6 occurred on or about June 13, 2018, in the Eastern District of Michigan. The Indictment also contained Forfeiture Allegations.

On September 10, 2019, the defendant pleaded guilty, pursuant to a written Rule 11 Plea Agreement, to Counts 1 through 5 of the Indictment. As part of the plea process, and taking into account the government's assessment of defendant's potential for recidivism and the fact a within guideline sentence on the other counts would be sufficient but not greater than necessary to achieve the §3553(a) factors, the government agreed to dismiss Count 6 which required a mandatory two years consecutive to the other counts. .

As a result Woods faces a minimum guideline term of imprisonment of 24 months and a maximum statutory term of imprisonment of 20 years for Counts 1-4, and a maximum statutory term of 10 years imprisonment for Count 5, a fine of \$250,000 (per

count), a special assessment of \$500, and a maximum 3-year term of supervised release.

II. Sentencing Guideline Calculations and Relevant 3553(a) Factors

Congress has provided, through 18 U.S.C. § 3553(a), the relevant objectives and factors to be considered to impose a sentence “sufficient, but not greater than necessary.” Those objectives include: (1) the nature and circumstances of the offense, and the history and characteristics of the defendant; (2) the need for a sentence to reflect the basic aims of sentencing (including retribution, deterrence, incapacitation, and rehabilitation); (3) the kinds of sentences legally available; (4) the Sentencing Guidelines; (5) Sentencing Commission policy statements; and (6) the need to avoid unwarranted sentencing disparities (nationwide) among defendants with similar records found guilty of similar conduct. But sentencing starts with the calculation of the Guidelines range to promote the sentencing goals of Congress, namely to “provide certainty and fairness in meeting the purposes of sentencing, while avoiding unwarranted sentencing disparities[.]” *United States v. Booker*, 543 U.S. 220, 264 (2005).

A. Guidelines Calculation

The parties' guideline calculations is consistent with the Probation Department's calculation. The guideline range is based, in part, on the loss amount in paragraph 26. Probation and the government used the \$500 floor for each access device (*i.e.*, each stolen credit card) to avoid inflating the loss. *See* USSG § 2B1.1, cmt. n.3.(F)(i). Technically, the government could have asked for a significantly higher loss. Indeed, Section 2B1.1 directs the Court to use the greater of the actual loss or the *intended loss*, and many courts in this type of case apply the aggregate credit limit of each stolen account in calculating the intended loss. *See, e.g., United States v. Alli*, 444 F.3d 34, 38–39 (1st Cir. 2006).

According to Experian, the average credit limit in 2017 was \$6,354 per card. In 2018, it was \$6,506.

(<https://www.experianplc.com/media/news/2019/state-of-credit-examines-credit-scores-decade-after-financial-crisis/>).

Even using a conservative \$6,000 limit per account would make the intended loss \$96,000, which would increase Woods's guidelines offense level up two levels from 6 to 8. The government does not ask for

this higher loss amount; it simply notes it as a point of reference why the guidelines are not inflated, but quite fair.

B. Section 3553(a) Factors

i. Nature of the Offense

This is not just a simple property offense. Credit card fraud is a rampant problem too often ignored by police focusing on violent offenses. In fairness, in the hierarchy of crimes, credit card fraud is less egregious than murder, sexual assault, or armed robbery. But Woods sought to exploit this view to their advantage—knowing that police have to focus much of their time on violent crime and drug trafficking, he turned to credit card fraud to avoid the attention of law enforcement. However, his rampant posts still attracted law enforcement scrutiny. Plus, Woods likely knew that, if arrested, the penalty would be significantly lower.

But the problem is that the money allegedly generated by Woods's fraud was so large that it attracted attention not from police, but from robbers. This led to Woods being shot and robbed as others tried to muscle in on Woods's purported riches. In other words, even though credit card or wire fraud are not "violent," the riches attained causes

violence. Plus, credit card fraud, in and of itself, impacts each and every member of society independent of this violence.

ii. History and Characteristics of the Defendant

Hill is 26 years old. He is uneducated, in that he dropped out of high school and does not have his GED. But despite this, he engaged in a wire fraud scheme extensively for over a year.

iii. Seriousness of the Offense

Successful credit card fraud is a serious crime that affects not only the account holders, but all of society. Victims suffer monetary damages and must prove that they did not, in fact, make the charge(s) to get reimbursed. But this process is lengthy, and it often involves temporary damage to their credit scores. Some reports indicate it can take hundreds of hours to undo the damage. *See* Madeleine Scinto, *Beware: Credit Card Fraud Will Pound Your Score*, BUSINESS INSIDER, Nov. 1, 2011, <http://www.businessinsider.com/beware-credit-card-fraud-will-pound-your-credit-score-2011-11>.

The cost to society is enormous. There is over \$11 billion in credit card fraud each year. Retailers and banks spend billions each year to combat credit card fraud, and yet there is still widespread fraud in the

United States. Ultimately, these costs are borne by everyone in the form of higher prices and increased fees. Adam Dolby, *Collateral Damage: The Effect of Card Fraud on Small Businesses, Customers and the Economy*, HUFFINGTON POST, April 24, 2014, http://www.huffingtonpost.com/adam-dolby/collateral-damage-the-eff_b_5206822.html

Locally, Michigan leads the nation in identity theft. Per capita, 175.6 people out of every 100,000 in the state will be the victim of identity theft. And this number is on the rise. There were 399,225 identity theft crimes in 2016—up nearly 60% over the last decade. *Michigan is #1 . . . in identity theft*, WLNS, April 14, 2017, <http://wlns.com/2017/04/14/michigan-is-1-in-identity-theft/>

iv. Promoting Respect for the Law and Providing Just Punishment

Woods showed his lack of respect for the law by his decision to persist in wire and credit card fraud. While Woods is not like other defendants who have lengthy criminal histories and multiple prior arrests, the fact that he flaunted his fraud online is striking and suggests a lenient sentence would not deter him specifically.

In terms of just punishment, the United States believes this case warrants a sentence of 28 months. Nationally, district courts vary from the applicable Guidelines range using the § 3553(a) factors in only 25% of fraud cases.¹ Typically, judges vary from the guidelines only when the loss amount is high, such as in white collar securities fraud cases. But that is not this case. This is a case of wire and credit card fraud and an example of pure greed.

v. Need for Deterrence

All of the above factors also implicate the need for a sentence to provide sufficient deterrence. Woods is young, but he shows no respect for the law or concern about his actions. This case provides an opportunity to deter him from future criminal conduct, and a minimal sentence of 28 months will reinforce the idea that he cannot commit this type of crime without consequence. Plus, if Hill is not stringently punished, it fails to deter his large social media following of other would

¹ United States Sentencing Commission, Sentences Relative to the Guideline Range by Selected Primary Offense Category (Fiscal Year 2016) 19, *available at* <http://www.ussc.gov/sites/default/files/pdf/research-and-publications/federal-sentencing-statistics/state-district-circuit/2016/6c16.pdf>.

be credit card fraudsters. other Bandgang cohorts under investigation or pending sentencing, who will view the federal court system as impotent like they already do the state system.

This case is one of many of my cases involving credit card or wire fraud. I prosecuted 12 similar cases involving 18 Bandgang members and associates—the vast majority of which were charged in this credit card and identity theft wave sweeping Michigan. One member of Bandgang, and a prolific swiper in his own right, Keeman Bridges, recently received a 154-month sentence before Judge Roberts in case 17-20769. Judge Roberts imposed a sentence at the bottom of Bridges’s guideline range because “[c]redit card fraud is becoming an epidemic in the Eastern District of Michigan as the crime is easy and there does not appear to be general deterrence.” Judge Roberts observed that lenient sentences in these cases do not appear to deter people.

III. Conclusion

For these reasons, the United States recommends a 28-month sentence of imprisonment.

Respectfully submitted,

Matthew Schneider
United States Attorney

/s/ Terrence R. Haugabook
Terrence R. Haugabook
Assistant U.S. Attorney
211 W. Fort Street, Suite 2001
Detroit, MI 48226
Phone: (313) 226-9157
Terrence.haugabook@usdoj.gov

Dated: January 6, 2020

Certificate of Service

I certify that on January 6, 2020, I electronically filed this Sentencing Memorandum, with the Clerk of the Court using the ECF system, which will send notification of such filing to the following attorney of the defendant:

Natasha Webster
Natasha_Webster@fd.org

/s/ Terrence R. Haugabook
Terrence R. Haugabook
Assistant U.S. Attorney
211 W. Fort Street, Suite 2001
Detroit, MI 48226
Phone: (313) 226-9157
Terrence.haugabook@usdoj.gov